WHAT IS CLAIMED IS:

1. A method for identification, comprising the steps of:

(a) generating system parameters G_1, G_2, P and $\hat{e}$ and storing the system parameters in a memory by a system administrator, wherein G_1 and G_2 are cyclic groups of order m, P is a generator on the cyclic group G_1, $\hat{e}$ is a bilinear map defined as

$$\hat{e}: G_1 \times G_1 \mapsto G_2;$$

(b) generating a private key $<a, b, c>$ and a public key v and storing the public key v in the memory by a prover or the system administrator, wherein a, b and c are randomly chosen in Z_m^* where Z_m^* is a multiplicative group of order m;

(c) generating random numbers $r_1, r_2, r_3 \in Z_m^*$ for obtaining an evidence (x, Q) and sending the evidence (x, Q) to a verifier by the prover;

(d) receiving the evidence (x, Q), selecting a randomly selected number ω □ Z_m^* to obtain a query R, storing the evidence (x, Q) and the randomly selected number ω in the memory and sending the query R to the prover by the verifier;

(e) receiving the query R, computing a temporary value S to obtain a response Y and sending the response Y to the verifier by the prover; and

(f) determining a legitimacy of the prover by employing the system parameters G_1, G_2, P and $\hat{e}$, the public key v, the evidence (x, Q) and the randomly selected number ω by the verifier.

2. The method of claim 1, wherein, in the step (b), the public key v is obtained by

$$v=\hat{e}(P,P)^{abc}$$

3. The method of claim 2, wherein, in the step (c), the evidence (*x*, *Q*) includes a first evidence value $x=\hat{e}(P,P)^{r_1 r_2 r_3}$ and a second evidence value

$$Q=r_1\,r_2\,r_3\,P$$

4. The method of claim 3, wherein, in the step (d), the query *R* is obtained by

$$R=\omega P$$

5. The method of claim 4, wherein, in the step (e), the temporary value *S* is obtained by $S=r_1 r_2 r_3 R$ and the response *Y* is obtained by

$$Y=abcP+(a+b+c)S$$

6. The method of claim 5, wherein the verifier determines the legitimacy of the prover by verifying

$$\begin{aligned}
\hat{e}(Y,P) &= \hat{e}(abcP+(a+b+c)S,P) \\
&= \hat{e}(abcP+(a+b+c)r_1 r_2 r_3 R,P) \\
&= \hat{e}(abcP+(a+b+c)r_1 r_2 r_3 \omega P,P) \\
&= \hat{e}((abc+(a+b+c)r_1 r_2 r_3 \omega)P,P) \\
&= \hat{e}(P,P)^{abc+(a+b+c)r_1 r_2 r_3 \omega} \\
&= \hat{e}(P,P)^{abc} \cdot \hat{e}(P,P)^{(a+b+c)r_1 r_2 r_3 \omega} \\
&= \hat{e}(P,P)^{abc} \cdot \hat{e}(P,r_1 r_2 r_3 P)^{(a+b+c)\omega} \\
&= \hat{e}(P,P)^{abc} \cdot \hat{e}(P,Q)^{(a+b+c)\omega} \\
&= \hat{e}(P,P)^{abc} \cdot \hat{e}((a+b+c),PQ)^{\omega} \\
&= \hat{e}(P,P)^{abc} \cdot \hat{e}(aP+bP+cP,Q)^{\omega} \\
&= v \cdot \hat{e}(aP+bP+cP,Q)^{\omega}
\end{aligned}$$

7. A method for identification, comprising the steps of:

(a) generating system parameters G_1, G_2, P and $\hat{e}$ and storing the system parameters in a memory by a system administrator, wherein G_1 and G_2 are cyclic groups of order m, P is a generator on the cyclic group G_1, $\hat{e}$ is a bilinear map defined as

$$\hat{e}: G_1 \times G_1 \mapsto G_2;$$

(b) generating a private key <a_1, a_2, ... a_n> and a public key v and storing the public key v in the memory by a prover or the system administrator, wherein a_1, a_2, ... a_n are randomly chosen in Z_m^* where Z_m^* is a multiplicative group of order m;

(c) generating random numbers r_1, r_2, … $r_n \in Z_m^*$ for obtaining an evidence (x, Q) and sending the evidence (x, Q) to a verifier by the prover;

(d) receiving the evidence (x, Q), selecting a randomly selected number ω □ Z_m^* to obtain a query R, storing the evidence (x, Q) and the randomly selected number ω in the memory and sending the query R to the prover by the verifier;

(e) receiving the query R, computing a temporary value S to obtain a response Y and sending the response Y to the verifier by the prover; and

(f) determining a legitimacy of the prover by employing the system parameters G_1, G_2, P and $\hat{e}$, the public key v, the evidence (x, Q) and the randomly selected number ω by the verifier.

8. The method of claim 7, wherein, in the step (b), the public key v is obtained by $v = \hat{e}(P, P)^{a_1 a_2 \ldots a_n}$.

9. The method of claim 8, wherein, in the step (c), the evidence (x, Q) includes a first evidence value

$v = \hat{e}(P, P)^{r_1 r_2 \ldots r_n}$ and a second evidence value $Q = r_1 r_2 \ldots r_n P$.

10. The method of claim 9, wherein, in the step (d), the query R is obtained by

$$R = \omega P$$

11. The method of claim 10, wherein, in the step (e), the temporary value S is obtained by $S = r_1r_2\ldots r_nR$ and the response Y is obtained by $Y = a_1a_2\ldots a_nP + (a_1+a_2+\ldots+a_n)S$

12. The method of claim 11, wherein the verifier determines the legitimacy of the prover by verifying

$$\begin{aligned}
&\hat{e}(Y, P)= \hat{e}(a_1a_2\ldots a_nP + (a_1+a_2+\ldots+a_n)S, P)\\
&= \hat{e}(a_1a_2\ldots a_nP + (a_1+a_2+\ldots+a_n)r_1r_2\ldots r_nR, P)\\
&\qquad = \hat{e}(a_1a_2\ldots a_nP + (a_1+a_2+\ldots+a_n)r_1r_2\ldots r_n\omega P, P)\\
&\qquad = \hat{e}((a_1a_2\ldots a_n + (a_1+a_2+\ldots+a_n)r_1r_2\ldots r_n\omega)P, P)\\
&\qquad = \hat{e}(P, P)^{a_1a_2\ldots a_n+(a_1+a_1+\ldots+a_n)r_1r_2\ldots r_n\omega}\\
&\qquad = \hat{e}(P, P)^{a_1a_2\ldots a_n} \cdot \hat{e}(P, P)^{(a_1+a_1+\ldots+a_n)r_1r_2\ldots r_n\omega}\\
&\qquad = \hat{e}(P, P)^{a_1a_2\ldots a_n} \cdot \hat{e}(P, r_1r_2\ldots r_nP)^{(a_1+a_1+\ldots+a_n)\omega}\\
&\qquad = \hat{e}(P, P)^{a_1a_2\ldots a_n} \cdot \hat{e}(P, Q)^{(a_1+a_1+\ldots+a_n)\omega}\\
&\qquad = \hat{e}(P, P)^{a_1a_2\ldots a_n} \cdot \hat{e}((a_1+a_2+\ldots+a_n), PQ)^{\omega}\\
&\qquad = \hat{e}(P, P)^{a_1a_2\ldots a_n} \cdot \hat{e}(a_1P+a_2P+\ldots+a_nP, Q)^{\omega}\\
&\qquad = v \cdot \hat{e}(a_1P+a_2P+\ldots+a_nP, Q)^{\omega}.
\end{aligned}$$